

Re: Web Single Sign On

Source:

<http://www.derkeiler.com/Newsgroups/microsoft.public.dotnet.framework.aspnet.security/2007-02/msg00001.html>

- *From:* "news.microsoft.com" <anonymous@xxxxxxxxxxxxxxx>
 - *Date:* Thu, 1 Feb 2007 14:37:23 -0800
-

Thanks for the information. Can Microsoft ISA Server solve such issues ?

"Joe Kaplan" <joseph.e.kaplan@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message news:OX90E5ORHHA.1908@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx

You can't do this. The way integrated Windows auth (IWA) works is that your IIS site is configured to require IWA and sends a 401.1 response to the browser with an instruction to authenticate via IWA (a www-authenticate header with "negotiate" and/or "NTLM" in the header).

The browser then sees this and knows that it is allowed to send its current Windows credentials to the server, so it does. If the server can authenticate these credentials, then it will and will return the content the user requested originally.

Since your server isn't in the domain, it won't understand the user's credentials.

The browser won't have any way to know to send a different set of credentials that the server might understand, so that won't happen either.

There are other types of SSO systems available like ADFS that integrate with IWA auth and can provide SSO like this, but ADFS doesn't do anything with Open LDAP. There may be some other SSO products out there that do...

Joe K.

Joe Kaplan-MS MVP Directory Services Programming
Co-author of "The .NET Developer's Guide to Directory Services Programming"

<http://www.directoryprogramming.net>

"quest" <anonymous@xxxxxxxxxxxxxxx> wrote in message news:%23k70oKNRHHA.4896@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx

My network environment consists of a domain with active directory(Win 2003 Server). My web application sits on IIS located outside the domain.

Re: Web Single Sign On

The web application is accessible through port 80 and without single sign on, requires user to enter username/password to gain access to the web application contents. A common identity has been constructed and stored in LDAP (open ldap- port 389 is open) located inside the domain. This common identity is the user's username used to logon to the domain/active directory.

To achieve single sign on, it is expected that when a user logons to the domain/active directory, he/she could access the web application (which sits on IIS outside the domain) without having to go through the logon process again. That means the user's credential (username) must be send over to the IIS which will use it to authenticate against LDAP sitting inside the domain. If the user is authenticated, the logon page will be by passed allowing user a direct access to the web application content.

My question:

1. How can this be achieved ? How does the browser know that it has to send the user's credential (username) to the IIS ?
2. Where and how does the browser get the user's credential (username in this case) since no logon page will be prompted to the user to logon the web application ?

Thanks.